

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

Jc784 U.S. PTO
09/735760
12/13/86

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

願年月日
Date of Application:

1999年12月20日

願番号
Application Number:

平成11年特許願第361221号

願人
Applicant(s):

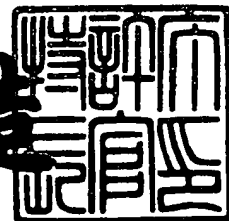
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 8月 4日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3062459

【書類名】 特許願

【整理番号】 9900272402

【提出日】 平成11年12月20日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 1/00 410

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 渡辺 一夫

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ソフトウェア使用制御方法とその装置

【特許請求の範囲】

【請求項 1】

ソフトウェア提供者側は、提供対象のソフトウェアと、該ソフトウェアに対応して用意されて該ソフトウェアを稼働する装置に接続する部材であって、前記接続された状態で該装置よりアクセス可能であり、内部に、前記対応するソフトウェアごとの所定の第 1 の情報が記憶されている部材とが配付されたソフトウェア使用者側に対して、前記部材に記憶されている前記第 1 の情報と照合する第 2 の情報を、公開鍵暗号方式の秘密鍵を用いて暗号化し、

前記暗号化した前記第 2 の情報を、前記ソフトウェア使用者側に送信し、

前記ソフトウェア使用者側は、前記伝達された暗号化された前記第 2 の情報を、前記公開鍵暗号方式の公開鍵を用いて復号し、

前記部材より前記第 1 の情報を読み出し、

前記読み出した前記第 1 の情報と前記復号した前記第 2 の情報とを照合し、

該照合が一致した場合に前記ソフトウェアの使用を可能とする

ソフトウェア使用制御方法。

【請求項 2】

前記ソフトウェア使用者側は、前記ソフトウェアの使用の許諾を求める際に、前記提供対象のソフトウェアおよび前記部材とともに配付される前記ソフトウェアを特定する所定の第 3 の情報を、前記ソフトウェア使用者側に伝達し、

前記ソフトウェア提供者側は、前記伝達された前記第 3 の情報に基づいて、前記ソフトウェア使用者側を特定し、該ソフトウェア使用者側に配付されている前記部材に記憶されている前記第 1 の情報と照合する前記第 2 の情報を検出し、

該第 2 の情報を前記暗号化する

請求項 1 に記載のソフトウェア使用制御方法。

【請求項 3】

前記第 1 の情報および前記第 2 の情報は、前記ソフトウェア使用者を特定する識別情報、または、前記配付されたソフトウェアまたは部材を特定する識別情報

であり、

前記第 2 の情報は、前記ソフトウェアおよび前記部材に添付されたパスワードである

請求項 2 に記載のソフトウェア使用制御方法。

【請求項 4】

前記ソフトウェアの使用を制御する処理を、前記ソフトウェア使用者側において前記ソフトウェアの使用を行なう都度行なう

請求項 3 に記載のソフトウェア使用制御方法。

【請求項 5】

前記ソフトウェアの使用を制御する処理を、ソフトウェア入手時、ソフトウェアのバージョンアップ時またはソフトウェアの利用期限の設定、更新時のいずれかを含む、予め定めた所定の時にのみ行なう

請求項 3 に記載のソフトウェア使用制御方法。

【請求項 6】

配付された使用対象のソフトウェアを記憶する記憶手段と、

所定のインターフェイス手段を介してアクセス可能に接続された部材であって、前記記憶しているソフトウェアごとの所定の第 1 の情報が記憶されている部材と、

前記記憶しているソフトウェアの使用の許諾を求める際に、当該ソフトウェアを特定する第 3 の情報を、ソフトウェア提供者側に送信する送信手段と、

前記ソフトウェア提供者側より伝送される、前記第 3 の情報に基づいて生成された前記第 1 の情報と照合する第 2 の情報を公開鍵暗号方式の秘密鍵を用いて暗号化された情報を受信する受信手段と、

前記受信した暗号化された第 2 の情報を、前記公開鍵暗号方式の公開鍵を用いて復号する復号手段と、

前記部材に記憶されている前記第 1 の情報と前記復号した前記第 2 の情報とを照合する照合手段と、

該照合が成功した場合に前記ソフトウェアを使用可能とする実行制御手段とを有するソフトウェア使用制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、たとえばコンピュータプログラムなどのソフトウェアの不正利用を防止し、適正な使用者のみ使用可能にするソフトウェア使用制御方法とその装置に関する。

【0002】

【従来の技術】

たとえばコンピュータプログラムなどのソフトウェアを頒布する際には、ソフトウェアの不正コピーや不正偽造を防止し、使用を許諾した適正な使用者にのみ使用を可能な状態で頒布することが重要である。

従来、このような不正利用対策としては、パスワードを利用する方法や、 dongle や IC カードなどを利用する方法がとられている。

前者は、ソフトウェアの起動時に各ソフトウェアごとのパスワードを入力しなければソフトウェアが有効に動作しないようにしたもので、ソフトウェア内で入力されたパスワードと予め登録されているパスワードとの照合を行なうことにより実現される。なお、このパスワードとしては、秘密鍵などが用いられている場合が多い。

【0003】

後者は、dongle や IC カードをソフトウェアとともに配付し、ソフトウェア起動時に、各ソフトウェアの識別子と、dongle や IC カードに記述されている識別子との照合を行なうものである。この識別子も、通常、秘密鍵などが用いられている。この方法においては、ソフトウェア内の秘密情報が解読されても、dongle や IC カードがなければソフトウェアを利用することはできず、より安全性の高い方法とすることができる。

【0004】

【発明が解決しようとする課題】

しかしながら、前述したパスワードを用いる方法では、本来は漏洩しないように管理されている筈のパスワード（秘密鍵）自体が、意図的に、あるいは、偶発的

に適正な利用者以外の者に伝わり、ソフトウェアが不正利用されてしまう可能性があり、また、実際にそのような不正利用も多く発生している。

また、dongleやICカードを用いる方法においても、そのdongleやICカードの偽造や複製が完全に不可能であるとは言い切れず、偽造や複製されソフトウェアが不正利用される可能性がある。また、この方法では、ソフトウェアのバージョンアップや変更などに合わせて、dongleやICカードを再配付しなければならず、処理が面倒である上に、コストもかかるという問題がある。

【0005】

したがって、本発明の目的は、より高い安全性でソフトウェアの使用を制御することができ、またバージョンアップや変更などにも容易に対応できるような、ソフトウェア使用制御方法を提供することにある。

また、本発明の他の目的は、より高い安全性でソフトウェアの使用を制御することができ、またバージョンアップや変更などにも容易に対応できるような、ソフトウェア使用制御装置を提供することにある。

【0006】

【課題を解決するための手段】

前記課題を解決するために、本発明のソフトウェア使用制御方法においては、ソフトウェア提供者側は、提供対象のソフトウェアと、該ソフトウェアに対応して用意されて該ソフトウェアを稼働する装置に接続する部材であって、前記接続された状態で該装置よりアクセス可能であり、内部に、前記対応するソフトウェアごとの所定の第1の情報が記憶されている部材とが配付されたソフトウェア使用者側に対して、前記部材に記憶されている前記第1の情報と照合する第2の情報を、公開鍵暗号方式の秘密鍵を用いて暗号化し、前記暗号化した前記第2の情報を、前記ソフトウェア使用者側に送信し、前記ソフトウェア使用者側は、前記伝達された暗号化された前記第2の情報を、前記公開鍵暗号方式の公開鍵を用いて復号し、前記部材より前記第1の情報を読み出し、前記読み出した前記第1の情報と前記復号した前記第2の情報とを照合し、該照合が一致した場合に前記ソフトウェアの使用を可能とする。

【0007】

また、本発明のソフトウェア使用制御方法は、配付された使用対象のソフトウェアを記憶する記憶手段と、所定のインターフェイス手段を介してアクセス可能に接続された部材であって、前記記憶しているソフトウェアごとの所定の第1の情報が記憶されている部材と、前記記憶しているソフトウェアの使用の許諾を求める際に、当該ソフトウェアを特定する第3の情報を、ソフトウェア提供者側に送信する送信手段と、前記ソフトウェア提供者側より伝送される、前記第3の情報に基づいて生成された前記第1の情報と照合する第2の情報を公開鍵暗号方式の秘密鍵を用いて暗号化された情報を受信する受信手段と、前記受信した暗号化された第2の情報を、前記公開鍵暗号方式の公開鍵を用いて復号する復号手段と、前記部材に記憶されている前記第1の情報と前記復号した前記第2の情報とを照合する照合手段と、該照合が成功した場合に前記ソフトウェアを使用可能とする実行制御手段とを有する。

【0008】

【発明の実施の形態】

本発明の一実施の形態について、図1～図6を参照して説明する。

本実施の形態においては、ソフトウェア販売会社が利用者にソフトウェアを販売し、利用者がそのソフトウェアを実際に使用する手順を説明することにより、本発明を説明する。

【0009】

まず、ソフトウェア販売会社が利用者にソフトウェアを販売する際の処理について、図1を参照して説明する。

まず、販売会社10は、ソフトウェアに、商品番号、ラベル名などそのソフトウェアを特定することのできるパスワード11を添付し、また、 dongle に、製品番号、dongle 番号、有効期日（恒久的に使用権限があるのか、利用期限付での使用権限か）など、ソフトウェアの使用形態に応じて決まる特定の識別情報12を内包させ、利用者20に配付する。

この時、販売会社10は、パスワード11と識別情報12および配付した利用者20との対応を管理しておく。特に、識別情報12に関しては、秘密の状態

管理しておく。

【0010】

次に、販売会社10は、販売会社のみで秘密にしておく公開鍵暗号方式による秘密鍵13と、それに対応する利用者用の公開鍵14を作成する。

そして、販売会社10は、各利用者に、利用者用の公開鍵14を伝達する。

販売会社が作成するこの秘密鍵13および公開鍵14の対は、各利用者ごとに共通としてもよいし、別のものを用意してもよい。共通にすれば、管理が容易となり、また、別にすれば、安全性が高まる。

また、この際に用いる公開鍵および秘密鍵は、十分に安全とされているデジタル署名方式の枠組みを使用する。

【0011】

次に、このような事前処理が終了した後に、使用者が実際に使用許諾を得て、ソフトウェアを使用する処理について、図2を参照して説明する。

まず、利用者20は、ライセンスを得ようとした場合、ソフトウェアに添付されているパスワードを、販売会社に送信する(21)。

販売会社は、利用者から受信したパスワードに基づいて、自ら管理している情報を検索して、各利用者ごとのソフトウェアの識別情報を検出する(22)。

次に、販売会社は、検出した識別情報を、販売会社の秘密鍵を用いて暗号化し、暗号化ライセンス情報を生成する(23)。

そして販売会社は、生成した暗号化ライセンス情報を、各利用者に送信する(24)。

【0012】

利用者は、この暗号化ライセンス情報を受信したら、ソフトウェアを起動し、ソフトウェア内の処理により、受信した暗号化ライセンス情報と dongle に内包している識別情報との照合を行なう(25)。

ソフトウェア内においては、まず、送信された暗号化ライセンス情報が公開鍵により復号され、利用者ごとのパスワードに対応したデータが得られる。

次に、dongle に内包してある識別情報と照合される。

そして、照合に合格すれば、ソフトウェアは有効に起動されて所望の処理を行

ない(26)、照合に失敗すればソフトウェアの実行を停止する(27)。

【0013】

このように、本実施の形態においては、 dongle に内包されている識別情報を用いてライセンスを行っており、このような dongle は、通常であれば利用者も知ることができないものである。したがって、ソフトウェアの使用を所望の形態に制御することができる。

また、ソフトウェアに受け渡す識別情報は、暗号化された形態となっており、この暗号化ライセンス情報を作成できるのは、秘密鍵を保持しているも販売会社のみである。したがって、仮に、識別情報を知り得たとしても、暗号化ライセンス情報を作成することは困難であり、よりセキュリティ高く、ソフトウェアの使用のライセンシーを制御できる。

【0014】

次に、前述した実施の形態のより具体的な例について説明する。

なお、以下の説明において、PN は購入時のソフトウェアに添付されている商品番号、DID は dongle ID 番号、PID はプロダクト ID 番号、CK はセクター秘密鍵、UK ユーザー公開鍵、 h は一方向性ハッシュ関数、(R, L) は暗号化ライセンス情報である。

なお、ここでは、Schnoor 署名を用いた場合について説明する。

【0015】

まず、販売会社での事前処理について、図3を参照して説明する。

まず、32ビット程度の素数 q を選び、次に、素数 q が $p-1$ の素因数となるような大きな1024ビット程度の素数 p を選び、得られた素数 p , q を、ソフトウェアおよび dongle に記録しておく(31)。

【0016】

この素数 q , p の選び方について、図4を参照して説明する。

まず、選択処理を開始したら(ステップS10)、たとえばラビン法などの確率的素数判定法を用いて32ビット程度の素数 q を選ぶ(ステップS11)。

次に、同じく確率的素数判定法により320ビット程度の素数 q_{-0} を選ぶ(ステップS12)。

次に、 $n = 1$ とおき（ステップ S 1 3）、同じく確率的素数判定法を用いてさらに素数 q_n を選ぶ（ステップ S 1 4）。

そして、 $a = 2 \times q_0 \times \cdots \times q_n$ を計算し（ステップ S 1 5）、その計算結果 a のサイズが 1 0 0 0 ビット程度の所定のビット幅に達しているか否かをチェックする（ステップ S 1 6）。

【0 0 1 7】

a が 1 0 0 0 ビットに足りない場合には（ステップ S 1 6）、 n を 1 カウントアップして（ステップ S 1 7）、ステップ S 1 4 以下の処理に戻る。すなわち、さらに次の素数 q_n を選び（ステップ S 1 4）、 $a = 2 \times q_0 \times \cdots \times q_n$ を計算し（ステップ S 1 5）、結果 a のサイズが所定のビット幅に達しているか否かをチェックする（ステップ S 1 6）。

このような処理を繰り返し、ステップ S 1 6 において結果 a のサイズが 1 0 0 0 ビット程度の所定のビット幅に達した場合には、 $p = q \times 2 \times q_0 \times \cdots \times q_{n+1}$ を計算し（ステップ S 1 8）、得られた値 p が素数であるか否かを確定的素数判定法により判定する（ステップ S 1 9）。

得られた値 p が素数で無い場合には、ステップ S 1 2 に戻り、値 p を得るためのステップ S 1 2 ～ステップ S 1 8 の処理を繰り返す。

ステップ S 1 9 において、得られた値 p が素数であれば、処理を終了する（ステップ S 2 0）。

【0 0 1 8】

次に、法 p に関する原始根 g を選び、 $h = g^{(p-1/q)} \bmod p$ を計算し、これもソフトウェアおよびドングルに記録しておく（3 2）。

この原始根 g を選ぶ処理について、図 5 を参照して説明する。

なお、 $p-1 = r_1 \times \cdots \times r_n$ とする。

まず、処理を開始したら（ステップ S 3 0）、 $1 < g < p$ となる g をランダムに選ぶ（ステップ S 3 1）。

次に、 $i = 1$ とおいて（ステップ S 3 2）、 $a = g^{(p-1/r_i)} \bmod p$ を計算し（ステップ S 3 3）、計算結果 a が $a \neq 1 \bmod p$ であるか否かをチェックする（ステップ S 3 4）。

【0019】

その結果、 $a = 1 \bmod p$ の場合は、ステップS31に戻り、再び g を選択する処理から開始する。

ステップS34において、 $a \neq 1 \bmod p$ だった場合には、全ての r_i に対してチェックを行なったか、すなわち $i = n$ か否かをチェックし（ステップS35）、 $i \neq n$ の時には、 i をカウントアップし（ステップS36）、ステップS33に戻り、次の r_i のチェックを行なう。

そして、全ての r_i に対してチェックを行なったら、その時に得られている g を原始根として、処理を終了する（ステップS37）。

【0020】

次に、 $0 < CK < q$ となるように、販売会社の秘密鍵 CK を任意に選ぶ（33）。この秘密鍵 CK は、販売会社だけの秘密として厳重に保管しておく。

【0021】

次に、利用者の鍵 UK を式1に基づいて計算し、この鍵 UK を利用者に知らせておく（34）。この利用者公開鍵 UK は、ソフトウェアの新規購入の時や、バージョンアップの時ごとに生成し、連絡する。

【0022】

【数1】

$$UK = h^{p-1-CK} \bmod p \quad \dots (1)$$

【0023】

次に、ソフトウェアに付属する dongle にソフトウェアの商品番号 PN （35）、これに対応する dongle ID 番号 DID 、および、プロダクトID番号 PID （36）を記録しておくとともに、これらを販売会社だけの秘密として厳重に保管しておく。

【0024】

そして、一方向性ハッシュ関数 H （ $1 \leq H$ の値域 $\leq q$ ）を用意し、これをソフトウェアおよびdongleに記録しておく（37）。

以上が、販売会社 10 で行なう事前処理の具体的内容である。

【0025】

次に、実際にライセンスを管理し、利用者側におけるソフトウェアの実行を制御する方法について、図 6 を参照して具体的に説明する。

まず、利用者は、ソフトウェアを購入した時、あるいは、利用期限を更新する時などに、商品番号 PN を販売会社に送信する (61)。

販売会社は、利用者より送信された商品番号 PN に基づいて、利用者のソフトウェアの DID および PID を獲得する (62)。

次に、販売会社は、乱数 k ($1 < k < q$) を生成し、式 2 に従って暗号化ライセンス情報 (R , L) を生成し、利用者へ送信する (63)。

【0026】

【数 2】

$$R = H(DID, PID, h^{\{k\}} \bmod p) \quad 0 < R < q \quad \dots (2)$$

$$L = CK \times R + k \bmod q$$

【0027】

利用者は、受信した暗号化ライセンス情報 (R , L) と商品番号 PN を用いて、また、 dongle から商品番号 PN に対応する DID, PID を読み込み、式 3 に示すような照合を行なう (64)。

【0028】

【数 3】

$$H(DID, PID, H^{\{L\}} \times UK^{\{R\}} \bmod p) = R \quad \dots (3)$$

【0029】

そして、式 (3) が成立すれば、正当なユーザーであることを確認し、プログラムを有効に動作させ (65)、不成立の場合は、プログラムを停止させる (6

6)。

このような具体的な処理により、前述した本実施の形態が実施できる。

【0030】

なお、本発明は本実施の形態に限られるものではなく、種々の改変が可能である。

たとえば、本実施の形態においては、コンピュータプログラムを頒布する場合におけるライセンス管理方法を例示して本発明を説明したが、いわゆるライブラリと言われるような任意のシステムにおけるデータ、機能的な構造を有するデータなど、プログラム以外の種々のデータの使用に対しても適用可能である。

また、コンピュータ以外の任意の機械、システムなどで使用される、それらプログラムやデータなどについても適用可能である。

【0031】

また、前述した具体例においては、Schnoor署名を用いる例を示したが、RSA署名、DSA署名、ElGamal署名、Fiat-Shamir署名、楕円曲線に基づく署名など、任意のデジタル署名方式を用いることができる。

また、本実施の形態においては、ソフトウェアとともに dongle を配付する例を示したが、ICカードなどでもよい。

【0032】

なお、前述した例においては、販売会社10、利用者20などの言葉を用いたが、実際に前述した処理が行なわれるのは、販売会社側の情報処理装置、利用者側の情報処理装置である。

【0033】

【発明の効果】

このように、本発明によれば、より高い安全性でソフトウェアの使用を制御することができ、またバージョンアップや変更などにも容易に対応できるような、ソフトウェア使用制御方法を提供することができる。

また、より高い安全性でソフトウェアの使用を制御することができ、またバージョンアップや変更などにも容易に対応できるような、ソフトウェア使用制御装置を提供することができる。

【図面の簡単な説明】

【図 1】

図 1 は、本発明の一実施の形態のプログラム配信システムの配信事前処理を説明するための図である。

【図 2】

図 2 は、本発明の一実施の形態のプログラム配信システムの処理を説明するための図である。

【図 3】

図 3 は、本発明の一実施の形態のより具体的な例のプログラム配信システムの配信事前処理を説明するための図である。

【図 4】

図 4 は、図 3 に示した処理において、素数 p を求める処理を説明するためのフローチャートである。

【図 5】

図 5 は、図 3 に示した処理において、原始根 g を求める処理を説明するためのフローチャートである。

【図 6】

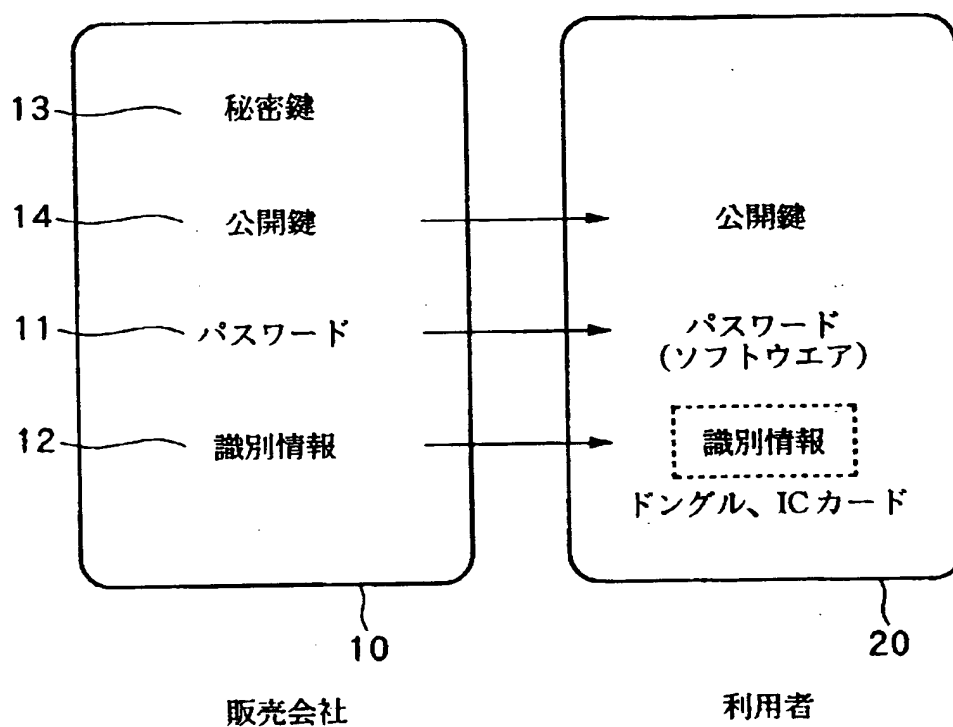
図 6 は、本発明の一実施の形態のより具体的な例のプログラム配信システムの処理を説明するための図である。

【符号の説明】

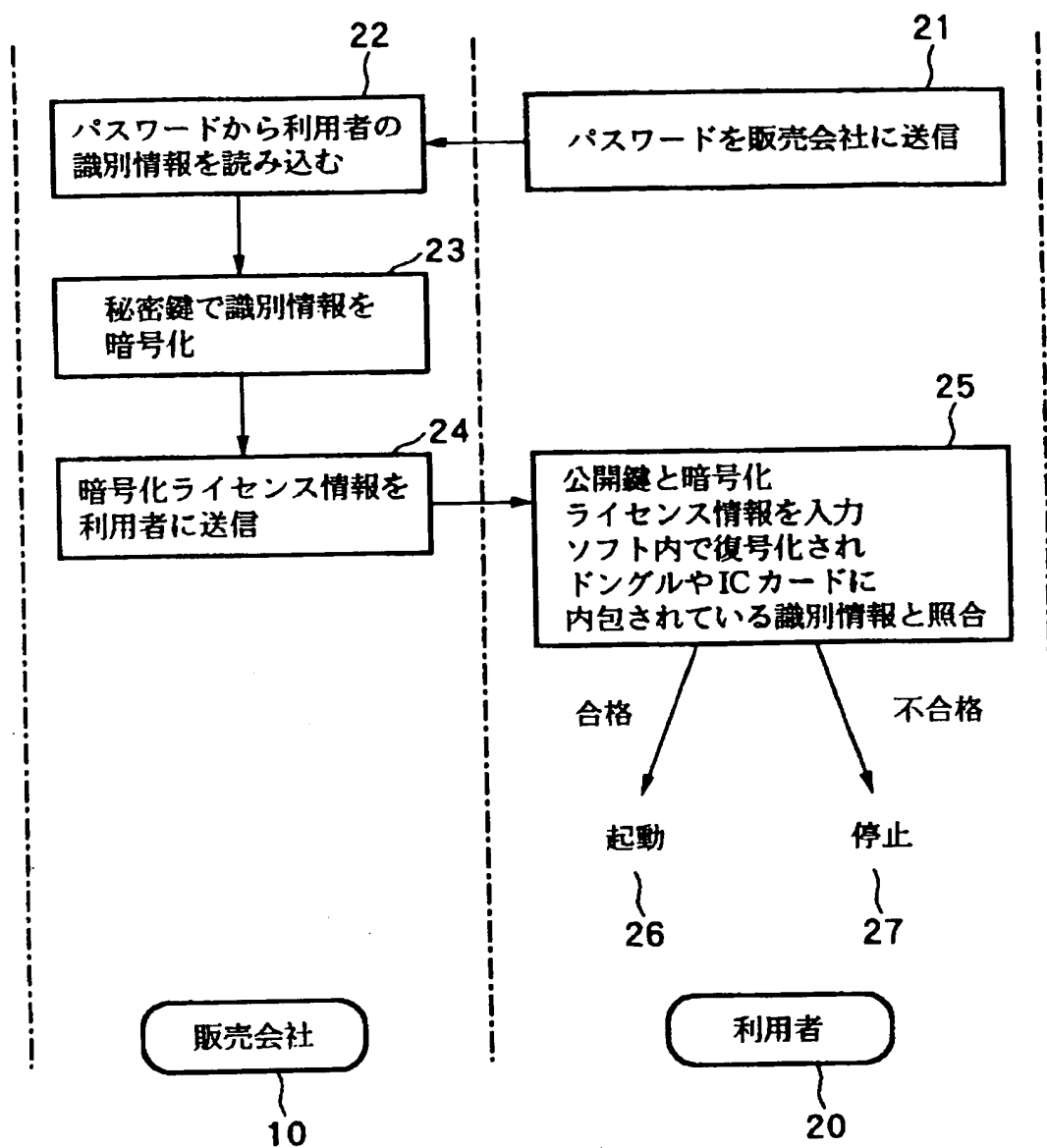
1 0 …販売会社、1 1 …パスワード、1 2 …識別情報、1 3 …秘密鍵、1 4 …公開鍵、2 0 …利用者

【書類名】 図面

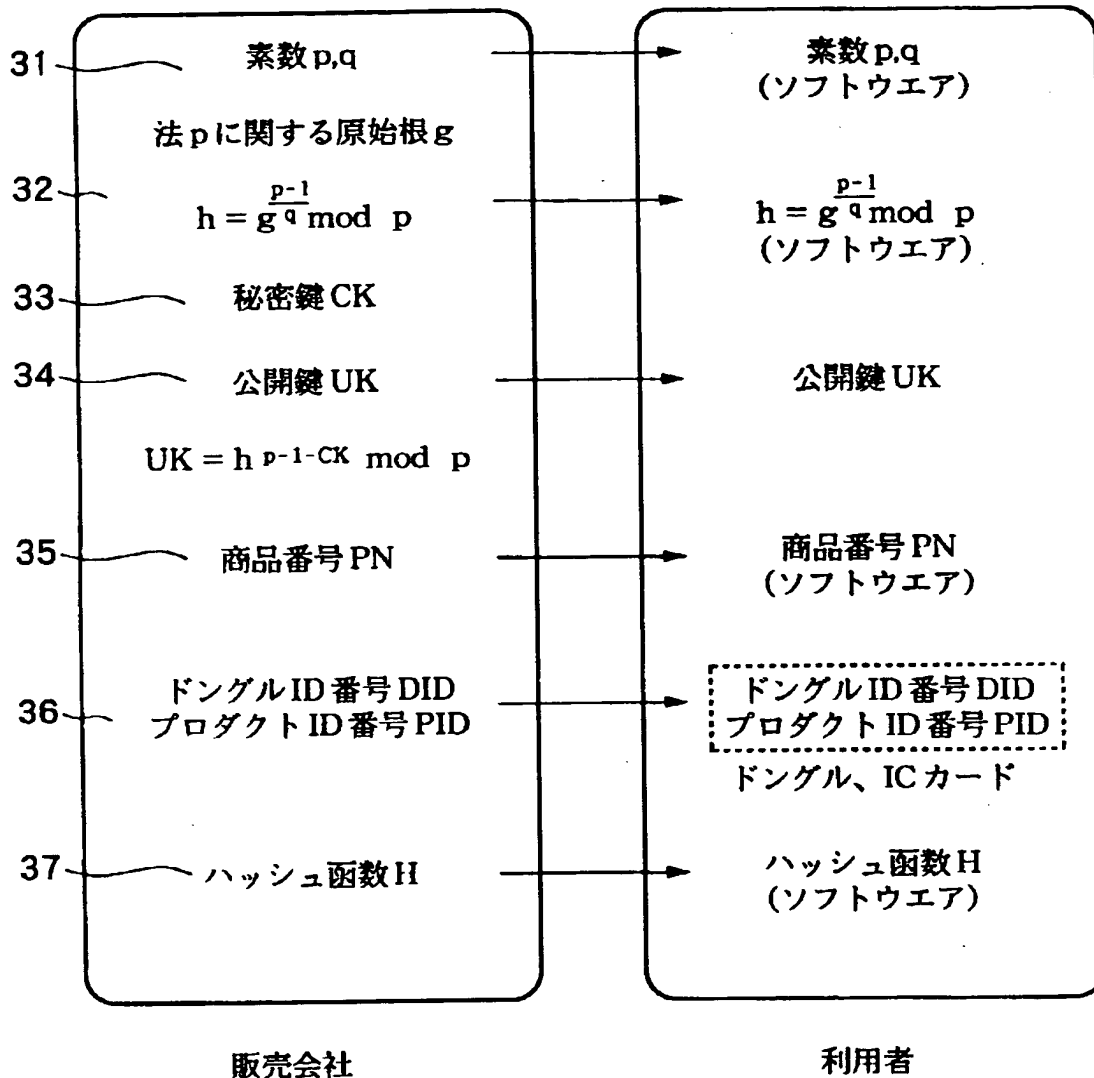
【図 1】



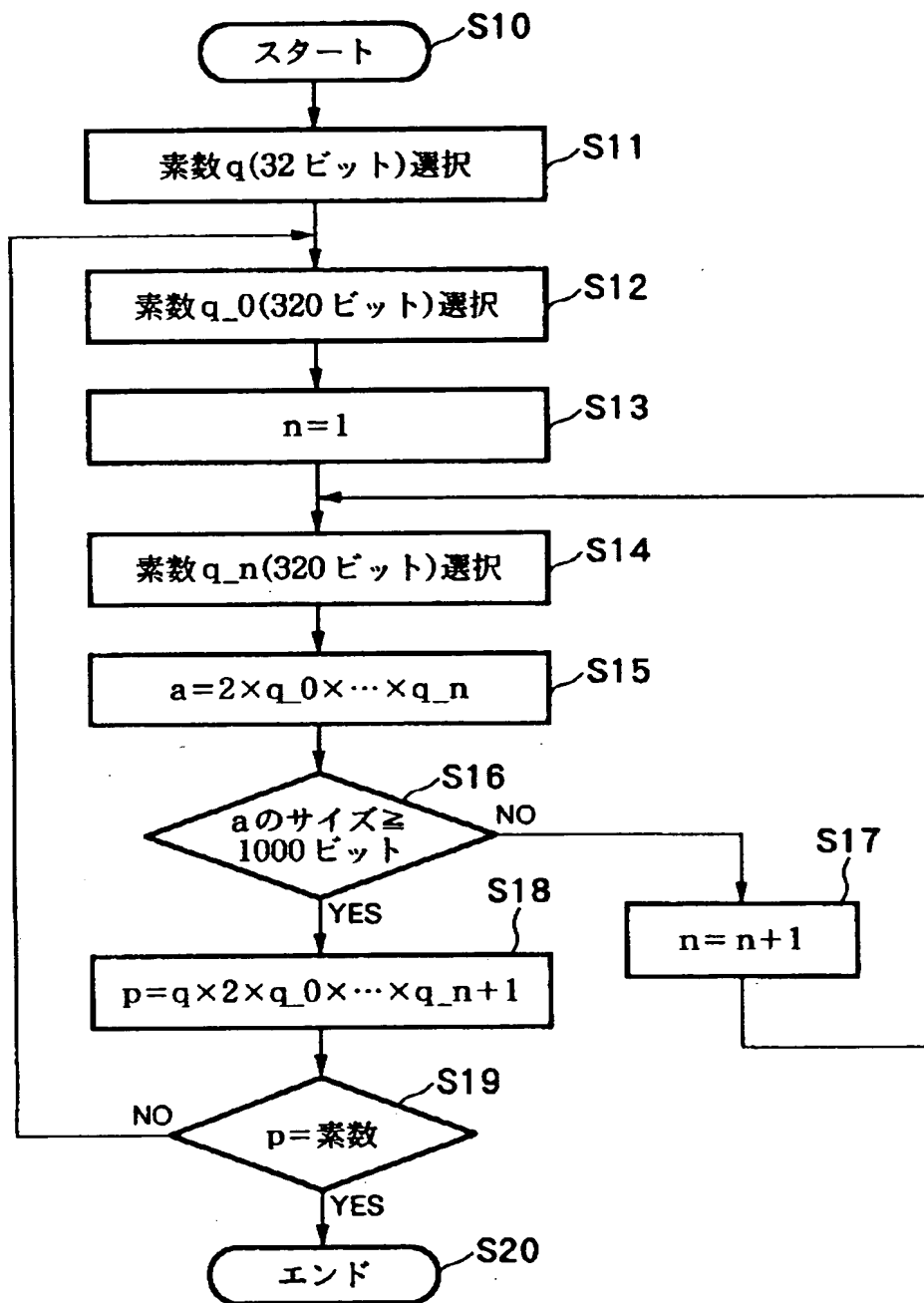
【図 2】



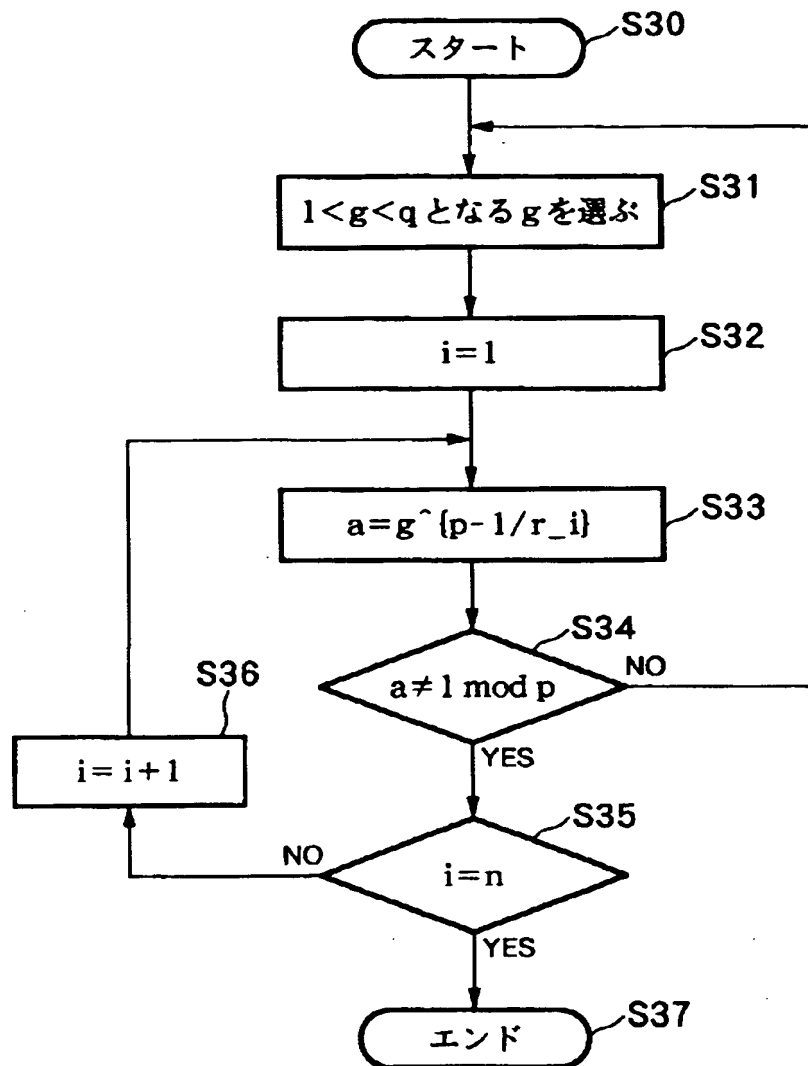
【図 3】



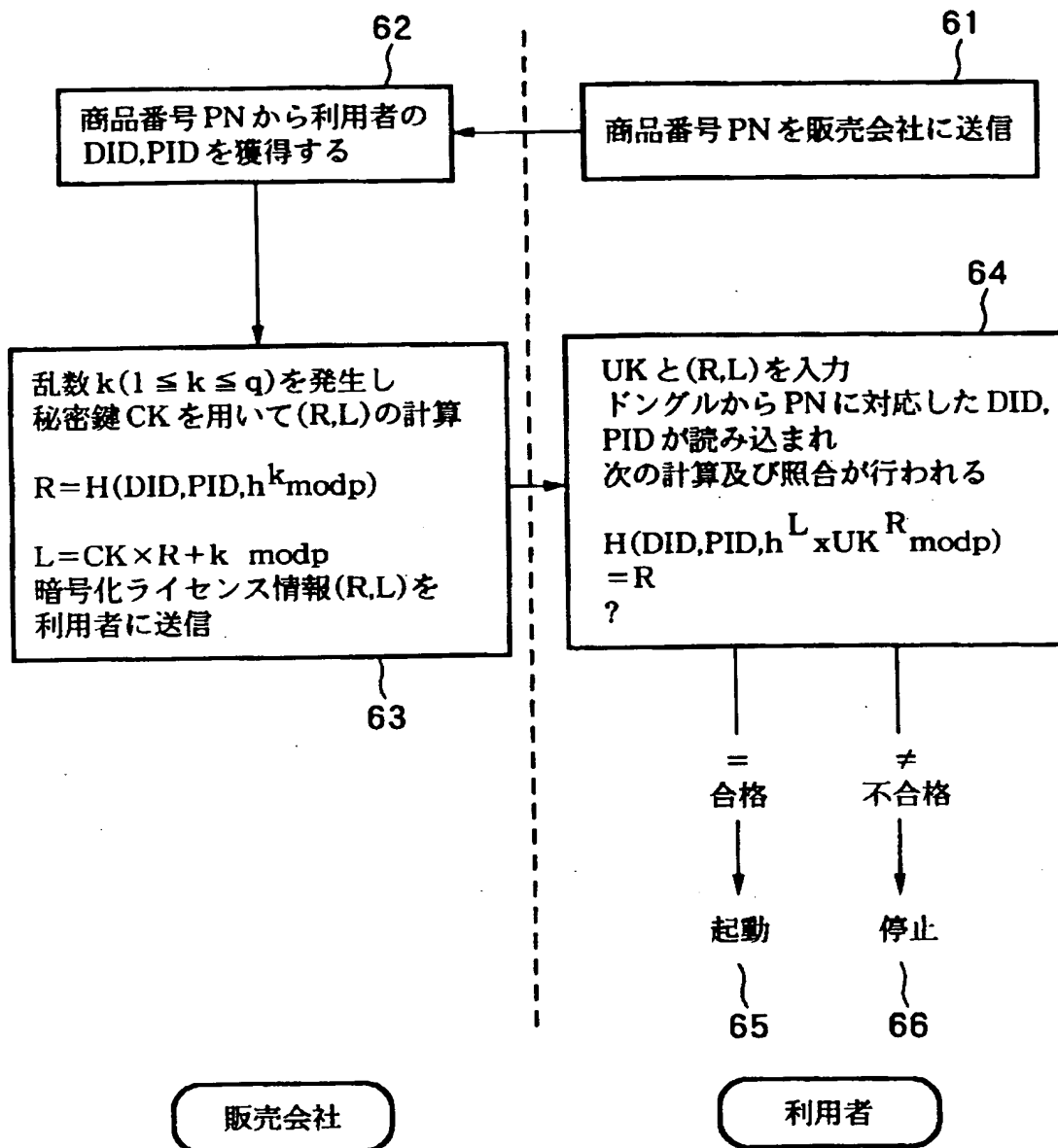
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 所望の形態でソフトウェアの使用を制御することができ、バージョンアップにも容易に対応できるようなソフトウェア使用制御方法を提供する。

【解決手段】 販売会社は、ソフトウェアにパスワードを添付し、dongleに識別情報を内包させ、利用者に配付する。また、秘密鍵と公開鍵を作成し、利用者に公開鍵を伝達する。利用者がライセンスを得ようとした場合、パスワードを販売会社へ送信する。販売会社は、パスワードに基づいて識別情報を検出し、秘密鍵を用いて暗号化し、暗号化ライセンス情報として利用者に送信する。利用者は、暗号化ライセンス情報を公開鍵により復号し、dongleに内包してある識別情報と照合する。照合に合格すれば、ソフトウェアは有効に起動され、失敗すればソフトウェアの実行を停止する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社